Title (en)

MODEL-BASED COMPUTER ATTACK ANALYTICS ORCHESTRATION

Title (de)

MODELLBASIERTE COMPUTERANGRIFFSANALYTIKORCHESTRIERUNG

Title (fr)

ORCHESTRATION ANALYTIQUE D'ATTAQUE INFORMATIQUE À BASE DE MODÈLE

Publication

EP 3264312 A1 20180103 (EN)

Application

EP 17173825 A 20170531

Priority

US 201615201186 A 20160701

Abstract (en)

Examples relate to model-based computer attack analytics orchestration. In one example, a computing device may: generate, using an attack model that specifies behavior of a particular attack on a computing system, a hypothesis for the particular attack, the hypothesis specifying, for a particular state of the particular attack, at least one attack action; identify, using the hypothesis, at least one analytics function for determining whether the at least one attack action specified by the hypothesis occurred on the computing system; provide an analytics device with instructions to execute the at least one analytics function on the computing system; receive analytics results from the analytics device; and update a state of the attack model based on the analytics results.

IPC 8 full level

G06F 21/55 (2013.01); **G06F 21/56** (2013.01); **H04L 29/06** (2006.01)

CPC (source: EP US)

G06F 16/90335 (2018.12 - EP US); **G06F 21/55** (2013.01 - EP US); **G06F 21/56** (2013.01 - EP US); **G06F 21/566** (2013.01 - EP US); **G06F 21/577** (2013.01 - US); **G06N 5/02** (2013.01 - US); **H04L 63/1408** (2013.01 - EP US); **H04L 63/1416** (2013.01 - EP US); **H04L 63/1425** (2013.01 - EP US); G06F 2221/034 (2013.01 - US)

Citation (search report)

- [XI] US 2016055335 A1 20160225 - HERWONO IAN [GB], et al
- [A] WO 2015128896 A1 20150903 - MITSUBISHI ELECTRIC CORP [JP] & EP 3113061 A1 20170104 - MITSUBISHI ELECTRIC CORP [JP]

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

EP 3264312 A1 20180103; US 10262132 B2 20190416; US 2018004941 A1 20180104

DOCDB simple family (application)

EP 17173825 A 20170531; US 201615201186 A 20160701